UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

26646 7590 06/08/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 06/08/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,181	06/15/2001	Joerg Schwenk	2345/152	3107

TITLE OF INVENTION: PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	09/08/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

26646 7590 06/08/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,181	06/15/2001	Joerg Schwenk	2345/152	3107

TITLE OF INVENTION: PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	09/08/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRUONG, THANHNGA B	2438	380-278000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,181	06/15/2001	Joerg Schwenk	2345/152	3107

26646 7590 06/08/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 06/08/2009

Determination of Patent Term Extension under 35 U.S.C. 154 (b)
(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	09/807,181	SCHWENK, JOERG	
	Examiner	Art Unit	
	THANHNGA B. TRUONG	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/2/07 and 7/5/07*.

2. ☒ The allowed claim(s) is/are *5,7 and 8*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 8/26/04
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438

DETAILED ACTION

1. Applicant's amendment filed on April 02, 2007 has been entered. Claims 1-8 are pending. Claims 1-4, 6 are cancelled; and claims 7-8 are newly added by the applicant.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

This examiner's amendment was given by the examiner to correct some typographical errors that present in claims 5 and 7, such as "the", or "said". If applicant disagrees with the correction, the applicant can file in the 312 amendment to make or revise the correction without changing the scope of the invention; otherwise, the 312 amendment will not be entered.

CLAIMS:

3. Please replace claim 5 as follows:

5. (Currently Amended) A process for secret transmission of a message by establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, as recited in comprising:

assigning the n subscribers respective leaves of a binary-structured tree which has a root, n leaves, is of depth [log2n] and has [[treenodes]] tree nodes;

for each one of the n subscribers, generating a respective secret, the respective secret being assigned to [[the]] each one of the n leaves to which the one of the n subscribers is assigned; and

establishing secrets consecutively in a direction of the root of [[the]] said tree for all k nodes of [[the]] said tree starting from the n leaves of [[the]] said tree across an entire hierarchy of [[the]] said tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common

secret being allocated to a common node so that [[a]] the common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of [[the]] said tree;

adding a new subscriber to the n subscribers of [[the]] said tree so that there are n+1 subscribers of [[the]] said tree, the adding step including:

adding two new leaves as successors to a selected one of the n leaves of [[the]] said tree so that [[the]] a new binary-structure tree has n+1 leaves and is of depth [log 2(n+1)];

assigning the one of the n subscribers to whom the selected one of the n leaves is assigned one of the two new leaves and assigning the new subscriber to another one of the two new leaves, the selected one of the n leaves becoming [[a]] the common node for the two new leaves; and

starting from the new leaves in [[a]] the direction of the root of [[the]] said tree, establishing new secrets only in those of the tree nodes which lie within a framework of [[the]] said tree on a path from the two new leaves to the root of [[the]] said tree.

Please replace claim 7 as follows:

7. (New) A method of transmitting a message to a location, comprising:

establishing a common cryptographic key for n subscribers using Diffie-Hellman process;

encrypting the message with the common cryptographic key;

transmitting the encrypted message to the location,

wherein, the establishing the common cryptographic key includes:

assigning the n subscribers respective leaves of a binary-structured tree which has a root, n leaves, is of depth [log2n] and has [[treenodes]] tree nodes;

for each one of the n subscribers, generating a respective secret, the respective secret being assigned to [[the]] each one of the n leaves to which the one of the n subscribers is assigned; and

establishing secrets consecutively in a direction of the root of [[the]] said tree for all k nodes of [[the]] said tree starting from the n leaves of [[the]] said tree across an entire hierarchy of [[the]] said tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that [[a]] the common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of [[the]] said tree;

adding a new subscriber to the n subscribers of [[the]] said tree so that there are n+1 subscribers of [[the]] said tree, the adding step including:

adding two new leaves as successors to a selected one of the n leaves of [[the]] said tree so that [[the]] a new binary-structure tree has n+1 leaves and is of depth [log2(n+1)];

assigning the one of the n subscribers to whom the selected one of the n leaves is assigned one of the two new leaves and assigning the new subscriber to another one of the two new leaves, the selected one of the n leaves becoming [[a]] the common node for the two new leaves; and

starting from the new leaves in [[a]] the direction of the root of [[the]] said tree, establishing new secrets only in those of the tree nodes which lie within a framework of [[the]] said tree on a path from the two new leaves to the root of [[the]] said tree.

Please replace claim 8 as follows:

8. (New) The method as recited in claim 7, further comprising:

excluding a selected one of the n subscribers from [[the]] said tree, the excluding steps including:

removing a first one of the n leaves of [[the]] said tree to which the selected one of the n subscribers is assigned;

removing a second one of the n leaves, the second one of the n leaves sharing a common node with the first one of the n leaves, the common node with the first one of the n leaves becoming a new leaf assigned to the one of the n subscribers to which the second one of the n leaves is assigned; and

starting from the new leaf of [[the]] said tree in [[a]] the direction of the root of [[the]] said tree, establishing new secrets only in those of the tree nodes which lie within a framework of [[the]] said tree on a path from the new leaf to the [[tree root]] root of said tree.

Allowable Subject Matter

4. Claims 5, 7, and 8 are allowed. The following is an examiner's statement of reasons for allowance: the prior arts do not disclose a process or method for secret transmission of a message by establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, as recited in comprising:

assigning the n subscribers respective leaves of a binary-structured tree which has a root, n leaves, is of depth [log2n] and has tree nodes;

for each one of the n subscribers, generating a respective secret, the respective secret being assigned to each one of the n leaves to which the one of the n subscribers is assigned; and

establishing secrets consecutively in a direction of the root of said tree for all k nodes of said tree starting from the n leaves of said tree across an entire hierarchy of said tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that the common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of said tree;

adding a new subscriber to the n subscribers of said tree so that there are n+1 subscribers of said tree, the adding step including:

adding two new leaves as successors to a selected one of the n leaves of said tree so that a new binary-structure tree has n+1 leaves and is of depth [log 2(n+1)];

assigning the one of the n subscribers to whom the selected one of the n leaves is assigned one of the two new leaves and assigning the new subscriber to another one of the two new leaves, the selected one of the n leaves becoming the common node for the two new leaves; and

starting from the new leaves in the direction of the root of said tree, establishing new secrets only in those of the tree nodes which lie within a framework of said tree on a path from the two new leaves to the root of said tree, as set forth in claims 5 and 7.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The central

fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438

TBT
May 24, 2009